NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

Analýza benefitov vyplývajúcich z implementácie NP: Detekcia zraniteľnosti koncových obslužných bodov

Projekt	Detekcia zraniteľnosti koncových obslužných bodov
Verzia dokumentu	1.0
Dátum vydania	12.07.2021
ID dokumentu	20210712_Analýza Benefitov NP Detekcia zraniteľnosti koncových obslužných bodov_v10
Autor	Peter Garaj
Vlastník	NASES

Národná agentúra pre sieťové a elektronické služby
BC Omnipolis, Trnavská cesta 100/II, 821 01 Bratislava
tel: +421 2 3278 0700
e-mail: info@nases.gov.sk
web: www.nases.gov.sk

Denník zmien:

Dátum vydania	Verzia	Popis verzie a zmien oproti predošlej verzii	Autor zmeny
18.03.2021	0.1	Prvá (iniciálna) verzia dokumentu	Peter Garaj
10.6.2021	0.2	Druhá verzia dokumentu zapracovanie pripomienok SITVS MIRRI SR zo dňa 8.9.2021	Peter Garaj
12.07.2021	1.0	Schválenie dokumentu RV	Michal Seliga

Obsah

Obsah

Zoznam skratiek a pojmov

ID	POJEM/SKRATKA	VYSVETLENIE
1	NASES	Národná agentúra pre sieťové a elektronické služby
2	UPVS	Ústredný portál verejnej správy
3	Štúdia	Štúdia s názvom „The Total Economic Impact™ Of Microsoft Cloud App Security“ publikovaná medzinárodnou konzultačno-poradenskou spoločnosťou Forrester. (https://tools.totaleconomicimpact.com/go/microsoft/CloudAppSecurity/)
4	Inappsecurity/ Microsoft Cloud App Security	Aplikačné riešenie pre detekciu hrozieb na strane klienta a sieťovej infraštruktúry nachádzajúcej sa mimo organizácie. Toto riešenie je navrhované v rámci realizácie NP: Detekcia zraniteľnosti koncových obslužných bodov. Pričom Microsoft Cloud App Security je cloudové riešenie.
5	NP: Detekcia zraniteľnosti koncových obslužných bodov	Pripravovaný národný projekt v gescii Národnej agentúry pre sieťové a elektronické služby
6	CBA/ Cost Benefits Analysis	Dokument vypracovávaný na základe Metodického pokynu k spracovaniu biznis case a cost benefit analýzy informačných technológií verejnej správy

NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

Účel dokumentu

V súlade s *Vyhláškou č. 85/2020 Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o riadení projektov v znení neskorších predpisov* je v rámci prípravy národného projektu potrebné vypracovanie Projektového zámeru a súvisiacich príloh a dokumentov. Medzi tieto dokumenty patrí aj vypracovanie dokumentu pre prípravu a hodnotenie základných parametrov a postupov finančnej analýzy projektu v oblasti IT a analýzy jeho nákladov a prínosov tzv. CBA (Cost Benefits Analysis).

Cieľom tohto dokumentu je poukázať na finančné vyčíslenie benefitov, ktoré prinesie realizácia NP Detekcia zraniteľnosti koncových obslužných bodov a jedná sa o podporný dokument k dokumentu CBA.

Potreba vypracovania dokumentu vyplýva z nutnosti získania nenávratného finančného príspevku pre realizáciu projektu a ubezpečenie poskytovateľa, že projekt bude po ukončení financovania z prostriedkov štátneho rozpočtu alebo nenávratného finančného príspevku finančne udržateľný.

Východiská

Jedným z hlavných východísk tohto dokumentu je samotná plánovaná realizácia NP: Detekcia zraniteľnosti koncových obslužných bodov, ktorého cieľom je vybudovanie riešenia pre detekciu hrozieb na strane klienta a sieťovej infraštruktúry mimo prevádzkovateľa ÚPVS/ NASES.

Ďalším východiskom pre túto analýzu benefitov je publikovaná štúdia s názvom *„The Total Economic Impact™ Of Microsoft Cloud App Security“* od medzinárodnej konzultačno-poradenskej spoločnosti Forrester[1]. Predmetná štúdia pojednáva o celkovom ekonomickom dopade na používanie riešenia Microsoft Cloud AppSecurity, ktoré pomáha organizáciám po celom svete chrániť ich aplikácie proti rôznym druhom „cyber“ útokov prostredníctvom obdobného riešenia, ktoré plánuje NASES realizovať prostredníctvom NP Detekcia zraniteľnosti koncových obslužných bodov. V rámci realizácie predmetnej štúdie boli oslovené štyri organizácie, ktoré implementovali a používajú Microsoft Cloud AppSecurity/ „inappsecurity“ riešenia, z rôznych oblastí priemyslu. Formou vykonania „interview“ a na základe ich odpovedí a skúsenosti autori štúdie dospeli k nasledovným kľúčovým zisteniam:

- Zníženie času a úsilia v rámci monitoringu bezpečnostných hrozieb a odstránenia bezpečnostného incidentu o 80%
- Automatická eliminácia až 75% všetkých potencionálnych bezpečnostných hrozieb
- Zníženie pravdepodobnosti úniku dát o 40%

Do finančného výpočtu benefitov NP: Detekcia zraniteľnosti koncových obslužných bodov vstupujú aj dáta/údaje ako mzdová politika zamestnávateľa NASES, štatistiky bezpečnostných incidentov vedených Sekciou bezpečnosti NASES a štatistiky týkajúce sa biznis transakcií a počtu aktívnych el. schránok v rámci UPVS.

Na základe vyššie uvedeného, analýzu benefitov NP: Detekcia zraniteľnosti koncových obslužných bodov budeme vyčíslovať na základe nasledovných kvantitatívnych ukazovateľov:

- Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov (Arg A1)
- Zníženie času a úsilia na odstránenie vzniknutého bezpečnostného incidentu (Arg B2)
- Zníženie pravdepodobnosti úniku dát (Arg C3)

Referenčné obdobie tejto analýzy sú tri (3) roky. V rámci tejto analýzy počas obdobia troch rokov používame v prepočtoch konštantné údaje ako 300 000 „endpointov“, konštantný počet hodín alokovaných na monitorovanie bezpečnosti a vyhodnocovania bezpečnostných rizík, priemerný počet incidentov za rok, konštantnú celkovú mzdu zamestnancov a atď.

[1] Zdroj: https://tools.totaleconomicimpact.com/go/microsoft/CloudAppSecurity/

1. Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov

Vstupy:

- Mzdová politika zamestnávateľa NASES (priemerná celková cena práce zamestnanca je 25 EUR/hodina CCP);
- V prípade, ak by chcela organizácia vykonávať proaktívny monitoring a vyhodnocovanie bezpečnostných incidentov bez používania riešenia „inappsecurity“, len prostredníctvom svojich zamestnancov, tak štúdia uvádza, že je potrebných 90 hodín/týždenne na monitorovanie bezpečnostných hrozieb zamestnancami pri počte „endpointov“ 30 000. Realizáciou NP: Detekcia zraniteľnosti koncových obslužných bodov plánujeme monitorovať minimálne 300 000 „endpointov“, čo je 10-krát viac „endpointov“, ako sa pojednáva v štúdii, z toho dôvodu túto skutočnosť reflektujeme v rámci prepočtu nižšie;
- Štúdia uvádza, že implementovaním riešenia „inappsecurity“ dôjde k zníženiu času o 80% potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov v treťom roku používania (1. rok: 60%; 2. rok: 70%; 3. rok: 80%);

Výsledok:

- Na základe výpočtov uvedených nižšie v tabuľke č. 1 finančné vyčíslenie tohto benefitu predstavuje za referenčné obdobie troch rokov úsporu celkom **2 457 000,00 €**

Tabuľka č. 1 - Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov

ID	Popis	Prepočet	1. rok	2. rok	3. rok	Spolu
A1.1	Počet hodín alokovaných na monitorovanie bezpečnosti a vyhodnocovania bezpečnostných rizík (pred nasadením "inappsecurity")	900 hodín*52 týždňov (rok)	46 800	46 800	46 800	
A1.2	Redukcia potrebného času prostredníctvom "inappsecurity"	Údaj zo štúdie	60%	70%	80%	
A1.3	Priemerná hodinová mzda pracovníka bezpečnosti NASES (Celková cena práce)	CCP/hodina	25 €	25 €	25 €	
Arg A1	**Výsledok**	**A1.1*A1.2*A1.3**	**702 000,00 €**	**819 000,00 €**	**936 000,00 €**	**2 457 000,00 €**

2. Zníženie času a úsilia na odstránenie vzniknutého bezpečnostného incidentu

Vstupy:

- Mzdová politika zamestnávateľa NASES (priemerná celková cena práce zamestnanca je 25 EUR/hodina CCP);
- Expertným odhadom predpokladáme, že počet incidentov v rámci minimálne 300 tis. endpointov bude približne minimálne 2 000 bezpečnostných incidentov/ročne;
- Štúdia uvádza, že identifikácia a odstránenie „cloudového“ incidentu trvá približne 96 osobohodín;
- Štúdia uvádza, že „inappsecurity“ automaticky eliminuje až 75% bezpečnostných hrozieb;
- Štúdia uvádza, že „inappsecurity“ zníži potrebný čas o 80% ohľadne identifikácie a odstránenia bezpečnostného incidentu v treťom roku používania (1. rok: 60%; 2. rok: 70%; 3. rok: 80%);

Výsledok:

- Na základe výpočtov uvedených nižšie v tabuľke č. 2 finančné vyčíslenie tohto benefitu predstavuje za referenčné obdobie troch rokov úsporu celkom **13 320 000,00 €.**

Tabuľka č. 2 – Zníženie času a úsilia na odstránenie vzniknutého bezpečnostného incidentu

ID	Popis	Prepočet	1. rok	2. rok	3. rok	Spolu
B2.1	Počet chránených endpointov	Minimálny plánovaný počet endpointov vyplývajúci z NP: Detekcia zraniteľnosti koncových obslužných bodov	300 000	300 000	300 000	
B2.2	Minimálny predpokladaný počet incidentov/rok	Expertný odhad (incidenty/rok)/ Údaj zo štúdie	2000	2000	2000	
B2.3	Incidenty eliminované automaticky "inappsecurity"	2000incidentov*75%automatická eliminácia	1500	1500	1500	
B2.4	Nedetekované incidenty "inappsecurity"	2000incidentov*25%nedetekovaných incidentov	500	500	500	
B2.5	Počet hodín na zistenie a odstránenie nedetekovaných incidentov	Údaj zo štúdie	96	96	96	

B2.6	Zníženie času na elimináciu nedetekovaného incidentu "inappsecurity"	Údaj zo štúdie	60%	70%	80%	
B2.7	Priemerná hodinová mzda pracovníka bezpečnosti NASES (Celková cena práce)	CCP/hodina	25 €	25 €	25 €	
Arg B2	**Výsledok**	**(750incidentov*96hodín*25EUR) + (250incidentov*96hodín*60%redukcia*25EUR)**	**4 320 000,00 €**	**4 440 000,00 €**	**4 560 000,00 €**	**13 320 000 €**

3. Zníženie pravdepodobnosti úniku dát

Vstupy:

- Štúdia uvádza, že priemerná finančná hodnota dáta je 10 $ (Kurz NBS ku dňu 18.3.2021 je 1.1907 EUR/USD; Prepočet: 10*1.1907=11,907 EUR);
- Štúdia uvádza, že pravdepodobnosť objemu úniku dát je 1,5%;
- Štúdia uvádza, že „inappsecurity“ dokáže znížiť pravdepodobnosť úniku dát o 40% v treťom roku používania (1. rok 30%; 2. rok 35%; 3. rok 40%);
- Počet biznis transakcií za rok 2020 v rámci ÚPVS bolo v objeme 34 201 478 dát (Oznámenia, Podania, Rozhodnutia, SkTalk2, Rozpracované, Odoslané)[2]
- Počet aktivovaných el. schránok k 31.12.2020 bolo v celkovom počte 584 722 (FO, PO a OVM)[3]

Výsledok:

- Na základe výpočtov uvedených nižšie v tabuľke č. 3 finančné vyčíslenie tohto benefitu predstavuje za referenčné obdobie troch rokov úsporu celkom **3 263 113,35 €.**

[2] Zdroj: https://www.slovensko.sk/sk/statistika-slovensko-sk
[3] Zdroj: https://data.gov.sk/dataset/upvs-schranky-aktivovane

Tabuľka č. 3 - Zníženie pravdepodobnosti úniku dát

ID	Popis	Prepočet	1. rok	2. rok	3. rok	Spolu
C3.1	Počet chránených dát	Cca 58 dát na používateľa ÚPVS (34 201 478 biznis transakcií(dát)/ 584 722aktívnych el. schránok)* 300 000 endpointov	17 400 000,00	17 400 000,00	17 400 000,00	
C3.2	Priemerná hodnota dáta (data asset)	Údaj zo štúdie	11,91 €	11,91 €	11,91 €	
C3.3	Celková hodnota dát	C3.1*C3.2	207 181 800,00 €	207 181 800,00 €	207 181 800,00 €	
C3.4	Pravdepodobnosť úniku dát bez "inappsecurity"	Údaj zo štúdie	1,50%	1,50%	1,50%	
C3.5	Potencionálny finančný dopad na únik dát	C3.3*C3.4	3 107 727,00 €	3 107 727,00 €	3 107 727,00 €	
C3.6	Zníženie pravdepodobnosti úniku dát implementovaním "inappsecurity"	Údaj zo štúdie	30%	35%	40%	

C3.7	Zníženie potencionálneho finančného dopadu na únik dát s "inappsecurity"	C3.5*C3.6	932 318,10 €	1 087 704,45 €	1 243 090,80 €	
Arg C3	**Výsledok**	**C3.7**	**932 318,10 €**	**1 087 704,45 €**	**1 243 090,80 €**	**3 263 113,35 €**

Zhrnutie/Sumár

Na základe vyššie uvedených prepočtov benefitov: *Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov (Arg A1), Zníženie času a úsilia na odstránenie vzniknutého bezpečnostného incidentu (Arg B2), Zníženie pravdepodobnosti úniku dát (Arg C3)* sme finančne vyčíslili celkový prínos NP: Detekcia zraniteľnosti koncových obslužných bodov v období troch rokov na celkovú sumu **19 040 113,35 EUR**.

Tabuľka č. 4 – Sumár vyčíslených benefitov

ID	Názov	1. rok	2. rok	3. rok	Spolu
Arg A1	Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov	702 000,00 €	819 000,00 €	936 000,00 €	2 457 000,00 €
Arg B2	Zníženie času a úsilia na odstránenie vzniknutého bezpečnostného incidentu	4 320 000,00 €	4 440 000,00 €	4 560 000,00 €	13 320 000,00 €
Arg C3	Zníženie pravdepodobnosti úniku dát	932 318,10 €	1 087 704,45 €	1 243 090,80 €	3 263 113,35 €
					19 040 113,35 €

Prílohy:

20210712_Prepočty_v10.xlsx